

(12) UK Patent Application (19) GB (11) 2 333 878 (13) A

(43) Date of A Publication 04.08.1999

(21) Application No 9901782.4

(22) Date of Filing 28.01.1999

(30) Priority Data

(31) 60072878

(32) 28.01.1998

(33) US

(31) 60097501

(32) 21.08.1998

(71) Applicant(s)

Citibank N.A.

(Incorporated in the USA)

**399 Park Avenue, New York, New York 10043,
United States of America**

(72) Inventor(s)

Alan Slater

(51) INT CL⁶

G07F 7/10, G06F 17/60

(52) UK CL (Edition Q)

G4T TBX

(56) Documents Cited

EP 0385400 A2

WO 95/26085 A1

US 5809143 A

US 5351296 A

(58) Field of Search

UK CL (Edition Q) G4T TBX

INT CL⁶ G06F 17/60, G07F 7/10, G07G 1/14

(74) Agent and/or Address for Service

Murgitroyd & Company

**373 Scotland Street, GLASGOW, G5 8QA,
United Kingdom**

(54) Abstract Title

Performing an online transaction using card information and PIN

(57) A method of performing a financial transaction between a purchaser 12 and a supplier 14 comprises creating an electronic instruction 15 containing encrypted card information (39, Figure 3), including card and bank account details, encrypted security information, including a PIN (40, Figure 3) for the card, and transaction amount information, and operating on the instruction using a secure mechanism 74 providing verification of the purchaser's identity and the instruction integrity. Preferably the instruction is created on a personal computer (50, Figure 3) and the secure mechanism involves a digital signature, a digital certificate, or encrypting the instruction. Preferably in operation the purchaser transmits the created instruction over the internet 16, by email or a WWW browser, to the supplier, who may append payment instructions 17 to the instruction and perform further encryption or security operations 76 on the instruction. The supplier sends, via the internet 18, the instruction to a financial institution having online ATM/POS access 24 to the bank accounts of both the purchaser 28 and supplier 34. The institution decrypts the instruction, verifies the instruction integrity and purchaser's account details, and transfers the required sum from the purchaser's account, accessed via the online ATM/POS link 30, 36 using the purchaser's card details and PIN, to the supplier's account. The institution then issues an authorisation message 32 to the supplier indicating the approval status of the transaction. A financial institution having online ATM/POS access to be used with such an instruction is also claimed.

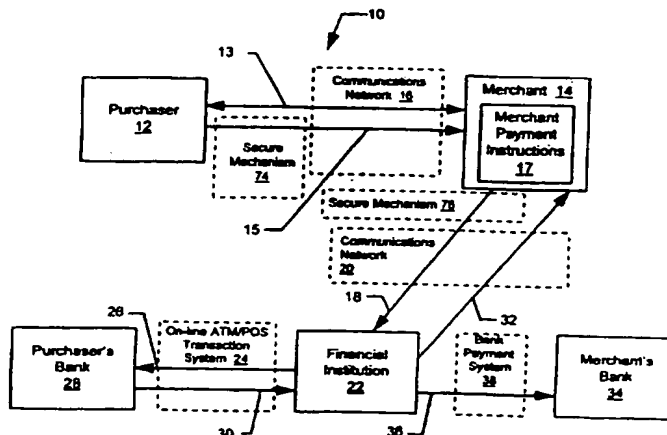


FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 333 878 A

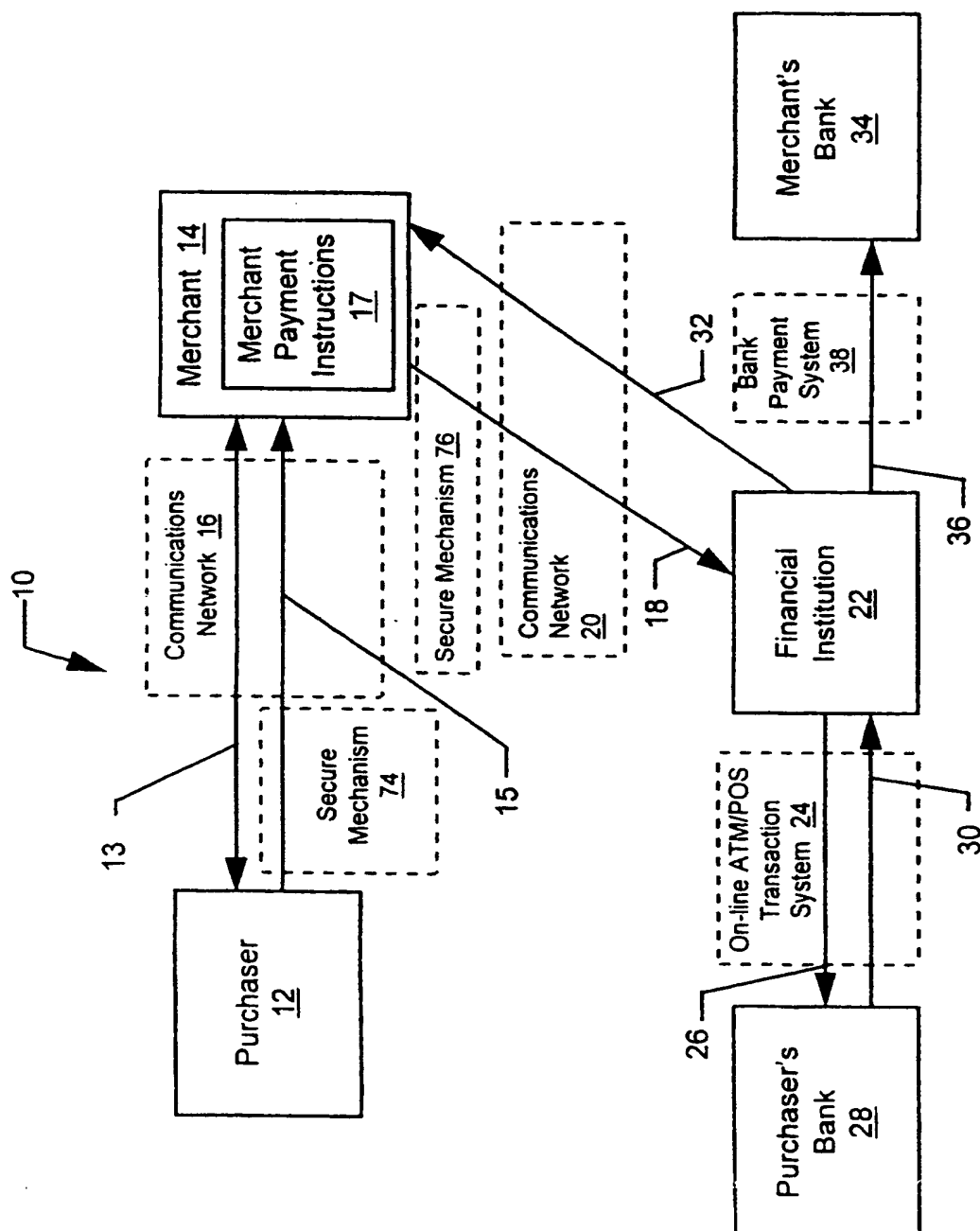


FIG. 1

FIG.2A

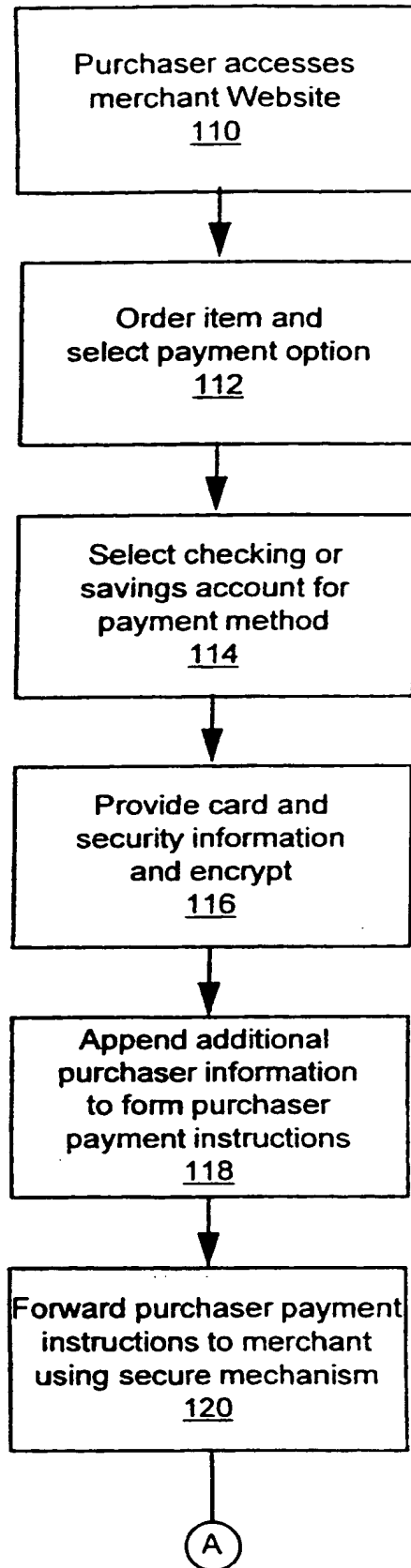
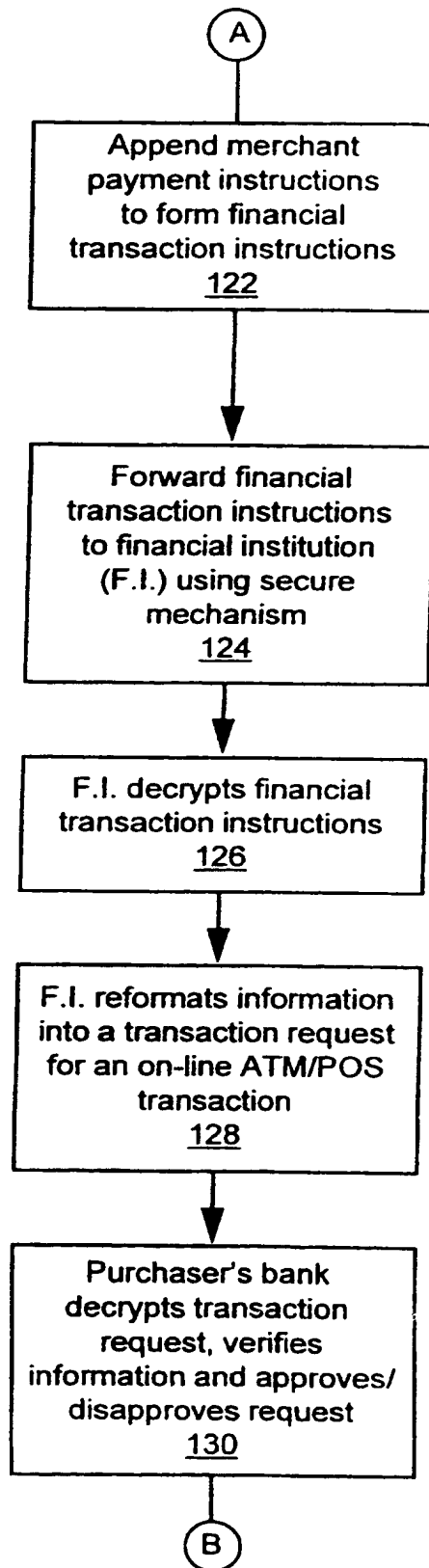


FIG.2B



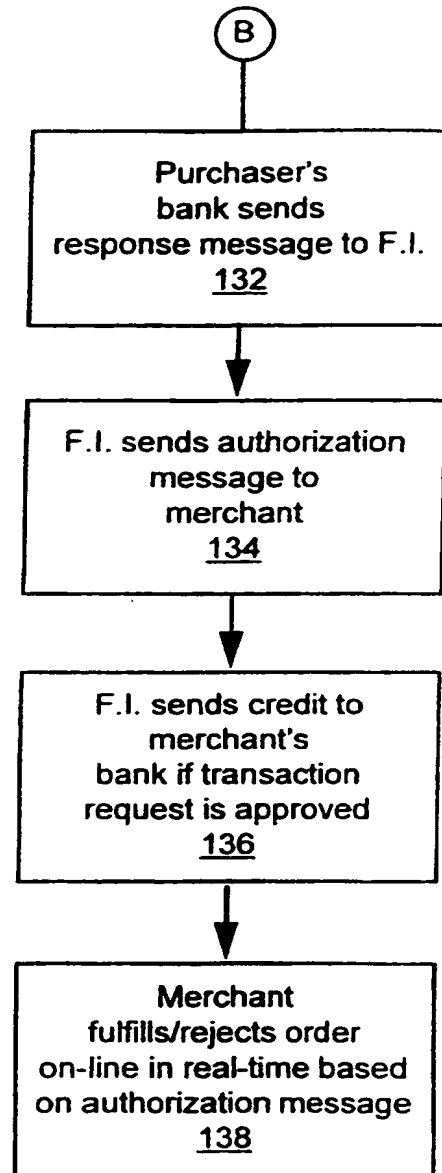


FIG. 2C

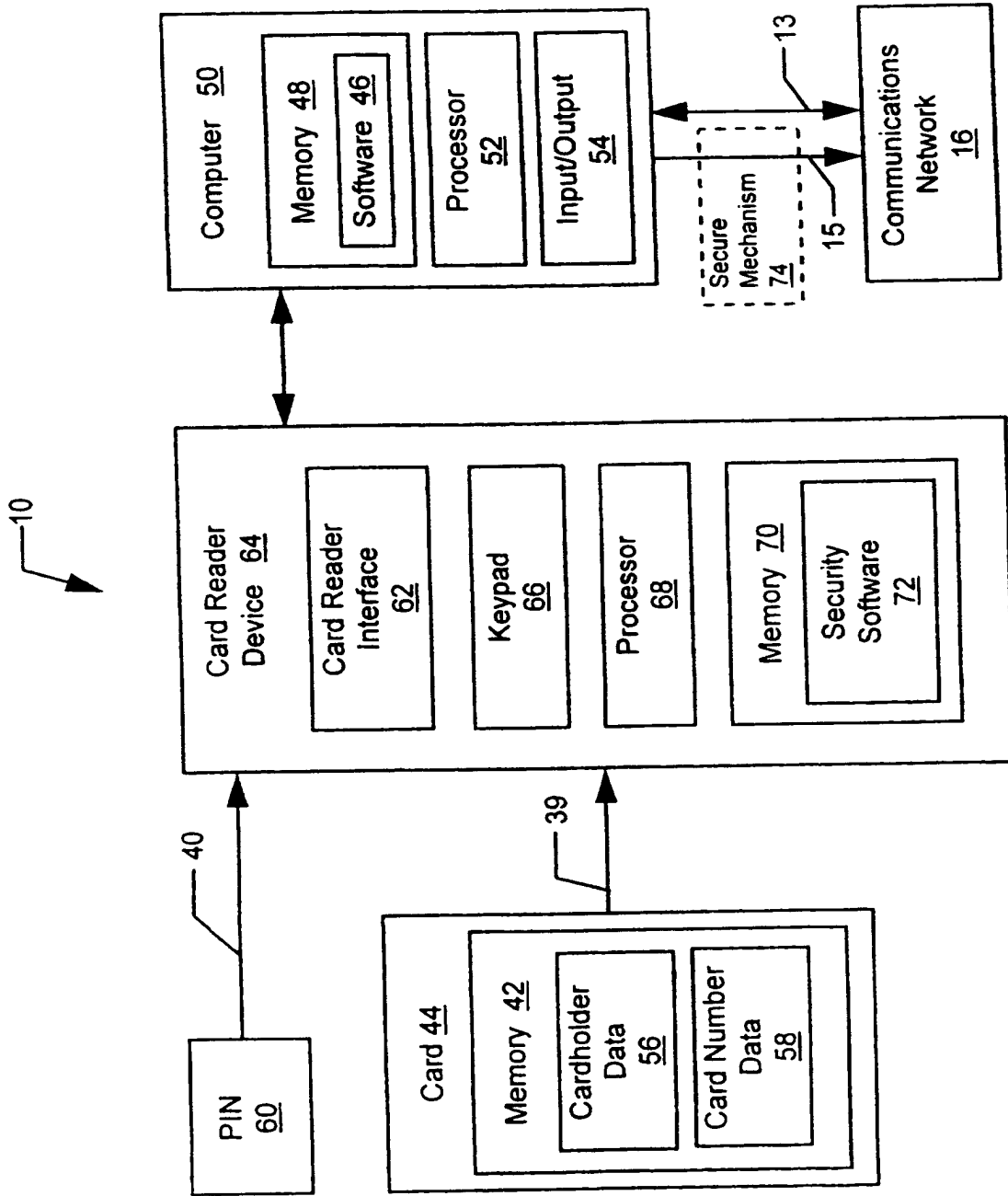


FIG.3

FIG.4A

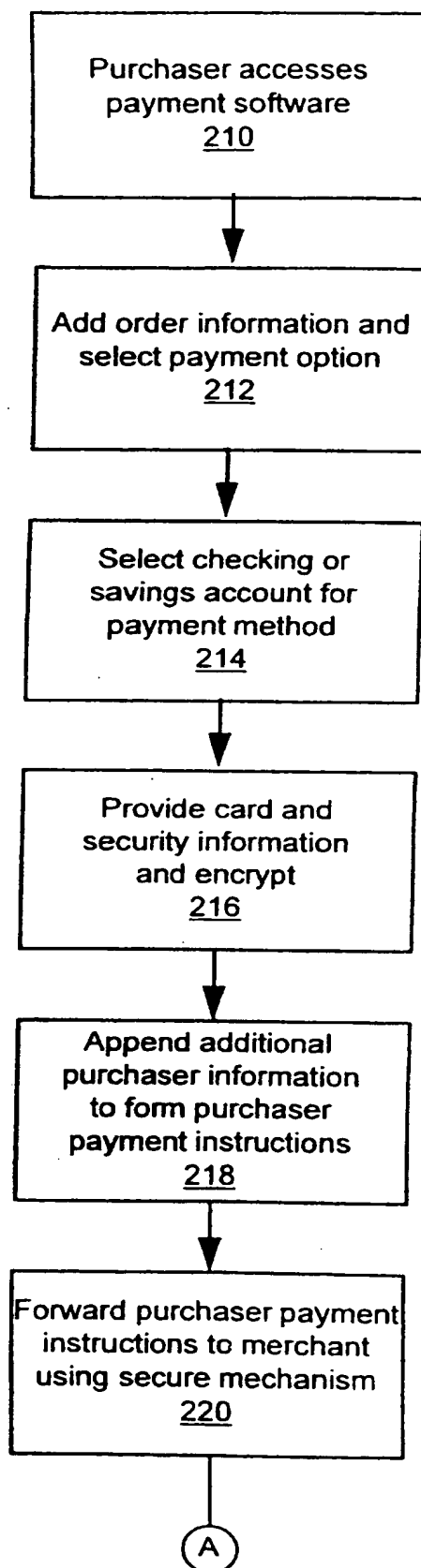
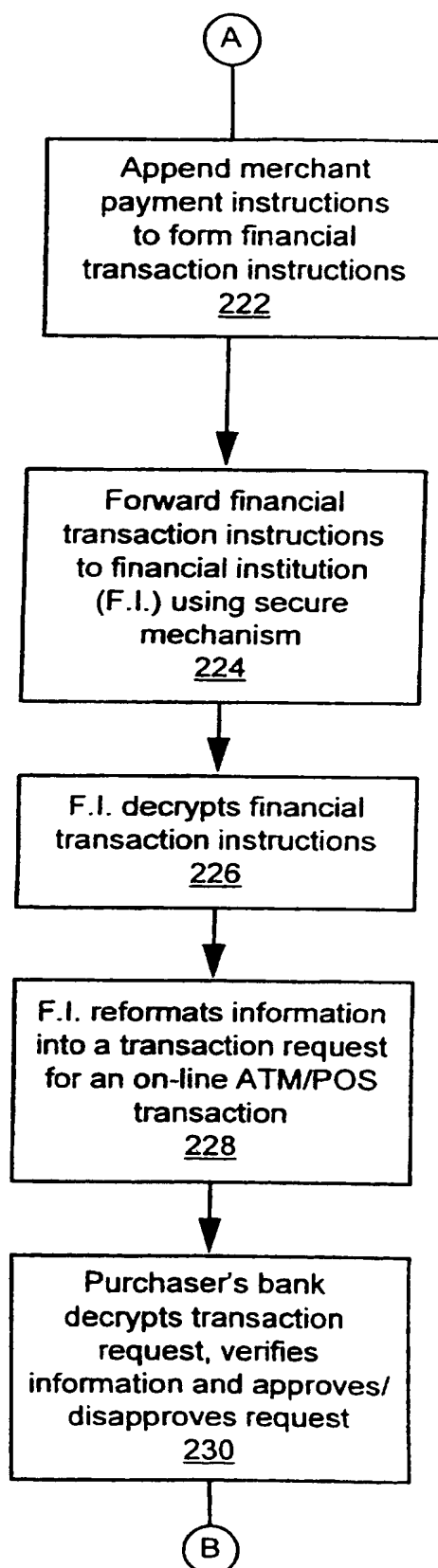


FIG.4B



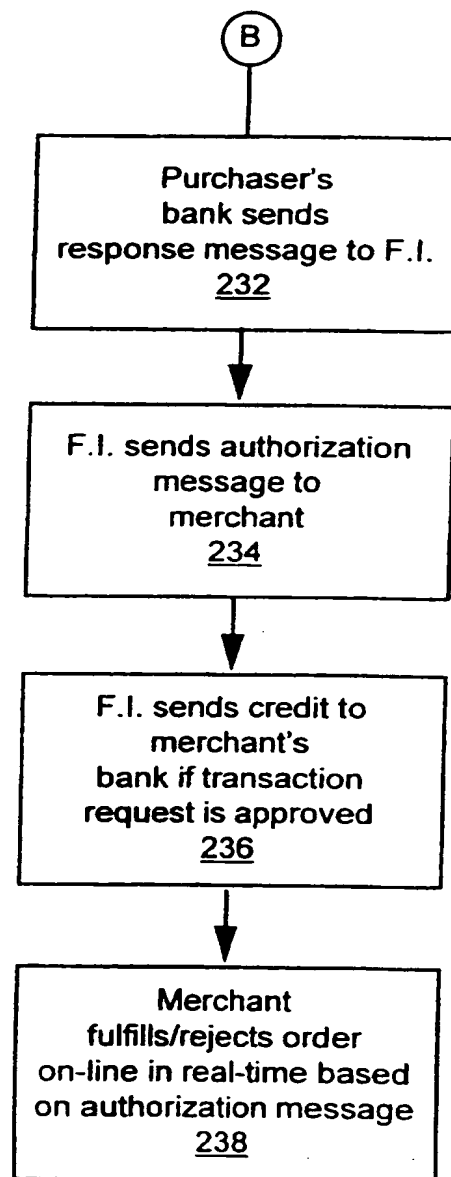


FIG.4C

1 **System And Method For Performing An Electronic**
2 **Financial Transaction**

4 **Cross-Reference to Related Applications**

5 This application claims the benefit of U.S.
6 Provisional Application No. 60/072,878 filed January
7 28, 1998 and U.S. Provisional Application No.
8 60/097,501 filed August 21, 1998.

10 **Background Of The Invention**

11 The present invention relates to electronic funds
12 transfer instruments, and more particularly, to
13 performing secure financial transactions over a public
14 access network using checking and savings account
15 funds.

17 With the increasing commercialization of the
18 Internet, new methods of performing secure and
19 verifiable payment transactions are desired. The most
20 common methods in use today, for example, require a
21 purchaser to enter credit card or non-PIN-based debit
22 card information and send it, unsecured or secured by
23 encryption, to a merchant. The merchant decrypts the
24 card information and uses it to complete the
25 transaction. This type of transaction is known as a

1 Mail Order Telephone Order (MOTO) transaction. MOTO
2 transactions are disadvantageous from a merchant
3 standpoint, however, because they are costly and risky.
4 A merchant's cost for performing a MOTO transaction may
5 be 5% or more of the entire transaction amount. MOTO
6 transactions are risky because the merchant has no idea
7 with whom they are actually dealing. Because a
8 personal identification number (PIN) is not required,
9 the only authorization-type of check that a merchant
10 can use in a MOTO transaction is to verify the mailing
11 address given by the purchaser with the issuing card
12 company's mailing address for the card number. Often,
13 the merchant must pay a fee to the card company to be
14 supplied with this mailing address information.
15 Further, the merchant, as opposed to the card company,
16 assumes liability for a shipment in a MOTO transaction
17 if no address confirmation is obtained.

18
19 For example, for a debit card linked to a credit
20 card account, a consumer does not need to enter a PIN
21 when they have a Visa® or Mastercard® logo on their
22 debit card. The transaction is performed like a credit
23 transaction, but the funds are taken out of their
24 checking account. That transaction goes through the
25 Visa/Mastercard credit network, and as a result the
26 merchant pays the 5% or more discount fee because the
27 transaction is treated like a credit card transaction
28 even though it winds up being charged to a checking
29 account. For the merchant, the transaction is settled
30 along with other credit card transactions, with the
31 settlement occurring usually the night of the
32 transaction, or the following day. For the purchaser,
33 the transaction may not be charged to their account for
34 several days.

35
36 A second type of POS transaction utilizes the

1 automated teller machine (ATM) network, making it a
2 completely on-line and real time transaction. This
3 type of on-line ATM/POS transaction is performed at ATM
4 machines or merchant POS terminals directly connected
5 to the ATM network. For this type of transaction, a
6 purchaser dips or swipes their ATM, debit or check
7 card, enters their PIN, and the network recognizes this
8 as an on-line ATM/POS transaction and routes it through
9 the same network that is used for ATM transactions. As
10 part of that routing process, the network is set up to
11 route the transaction according to a Bank
12 Identification Number (BIN) included in a Primary
13 Account Number (PAN), which is the embossed number on
14 the card. The embossed number on the card is also
15 stored on the magnetic stripe of the card, or for a
16 smart card, within the memory of the microcomputer chip
17 on the card. The BIN consists of the first six digits
18 of the embossed number, according to International
19 Standards Organization (ISO) standard number ISO 7812.
20 Further, ISO provides the BIN numbers worldwide to
21 insure that there is no duplication. The BIN tells the
22 ATM network how to route the transaction so that it
23 gets back to the purchaser's bank, and each bank that
24 accepts one of these on-line ATM/POS transactions has a
25 cross-reference between the embossed number and the
26 actual account number. The on-line ATM/POS transaction
27 creates an on-line authorization that verifies the card
28 number and PIN, and determines if the card is lost or
29 stolen or if the associated account is blocked.
30 Further, the associated bank account is checked to
31 determine if there are sufficient funds to cover the
32 transaction amount. The transaction is then settled
33 the same business day through the ATM networks.

34
35 An on-line ATM/POS transaction is beneficial to
36 both the purchaser and the merchant. For the purchaser

1 who would normally roll-over some or all of a credit
2 card transaction, the on-line ATM/POS transaction is
3 beneficial because it saves the purchaser from having
4 to pay finance charges. For the merchant, an on-line
5 ATM/POS transaction is beneficial because the cost to
6 the merchant for this type of transaction is based on a
7 fixed fee. The fixed fee is typically less than the
8 percentage of the transaction amount charged for credit
9 transactions, especially for transaction amounts over
10 about \$10-\$12 U.S. dollars. Thus, on-line ATM/POS
11 transactions are typically more desirable for the
12 merchant for these dollar amount transactions.

13

14 Currently, the ATM network is not set up to handle
15 the entry of a purchaser's actual account number into
16 an ATM or merchant POS terminal and have that account
17 number sent through the network. This is because the
18 actual account number is not in the proper format and
19 contains no routing instructions. Similarly, the ATM
20 network cannot handle the direct entry of a bank's
21 routing transit number followed by an account number,
22 for the same reasons. Even though the BIN provides
23 routing instructions, it is not the same number as a
24 bank routing transit number, which is used to route
25 paper checks, wire transfers and Automated Clearing
26 House transactions. Thus, transactions utilizing
27 merchant POS and ATM terminals are the only current
28 methods commercially available for an on-line, real
29 time financial transaction utilizing checking or
30 savings account funds.

31

32 In an effort to expand the available sources of
33 payment, methods have been developed to utilize
34 checking account funds to perform Internet
35 transactions. These methods allow the use of
36 "electronic checks" to perform transactions. One

1 example of such an electronic check is the "echeck"
2 process established by the Financial Services
3 Technology Consortium (FSTC). There are a number of
4 problems, however, associated with current electronic
5 check methods. For example, since the flow of the
6 current electronic check replicates the flow used for
7 paper checks, there is a delay between the time that
8 the electronic check is endorsed and the time that the
9 electronic check is approved for payment. This delay
10 may be one or more days. For example, the electronic
11 check transaction flow goes from the purchaser to the
12 merchant to the check service provider. The check
13 service provider issues a debit over the Automated
14 Clearing House (ACH) network or the Electronic Check
15 Processing (ECP) to the purchaser's account. The ACH
16 or ECP debit may take a couple of days to get to the
17 purchaser's bank, depending on how long the check
18 service provider holds on to the money to gain float
19 revenue. Also, there is the possibility that the ACH
20 or ECP debit may be returned (like a bounced check) if
21 there are not enough funds in the account. As a
22 result, the merchant typically must wait a number of
23 days to find out whether or not the funds are good,
24 thereby delaying fulfillment of the order. As such,
25 utilizing this type of electronic check creates
26 uncertainty for the merchant. as they are unsure if the
27 electronic check will be paid. Thus, despite the
28 transaction having the appearance to the purchaser of
29 being on-line and real time, it takes several days for
30 their account to be charged and for the transaction to
31 be completely processed.

32

33 Additionally, because the typical electronic check
34 process replicates the paper check process, the
35 transaction flow requires the merchant's bank to have
36 the electronic check capability. For a consumer to be

1 able to use this type of electronic check, however, the
2 consumer must be a member of a bank or financial
3 institution that offers this service. Over the next 5
4 to 10 years, however, only a few dozen financial
5 institutions are estimated to participate in issuing
6 electronic checks. Because of this limited
7 participation, the majority of purchasers will not have
8 access to electronic checks from the financial
9 institution with whom they have an account
10 relationship. Thus, in turn, the number of purchasers
11 that a merchant can attract and serve with an
12 electronic check is limited.

13

14 Additionally, for example, not only must the
15 purchaser be a member of a participating financial
16 institution, but the merchant must set up procedures
17 for these types of transactions to deal with the
18 limited number of participating financial institutions.
19 Due to the limited number of customers who would
20 utilize this payment method, a merchant may be
21 discouraged from expending the time and money to
22 establish such a system.

23

24 Another scheme requires the purchaser to deposit
25 funds into a trusted third party's account before the
26 purchaser can perform a transaction. This scheme is
27 fraught with inefficiencies. For example,
28 inefficiencies include the time wasted as purchaser
29 must plan ahead in order to deposit the funds, and also
30 the time wasted in finding a third party mutually
31 trusted by the purchaser and the merchant. Thus, the
32 use of trusted third parties is not desirable for on-
33 line, real time transactions.

34

35 Further, with the Internet serving a worldwide
36 market, there is a desire for allowing a purchaser

1 using one currency to perform an on-line, real time
2 financial transaction with a merchant using another
3 currency. The ATM network discussed above allows this
4 type of transaction to occur. For example, a United
5 States citizen traveling in a foreign country can
6 utilize their ATM debit card in a local ATM to get a
7 designated amount of the local currency. The
8 functionality exists within the ATM network to convert
9 the amount of local currency obtained into a
10 corresponding amount of United States dollars and debit
11 the appropriate amount.

12

13 Currently, there is a need for low cost access to
14 checking and savings accounts to perform financial
15 transactions over the Internet. There is no current
16 mechanism, however, that connects the ATM network to
17 purchasers on the Internet. Most purchasers access the
18 Internet from remote locations, such as personal
19 computers at home or at a business. Meanwhile, access
20 to the ATM network is typically provided only through
21 ATM machines and POS merchant terminals directly
22 connected to the network. Thus, there is currently no
23 mechanism that allows purchasers and merchants using
24 the Internet or electronic mail the real-time, on-line
25 ATM/POS transaction functionality provided by the on-
26 line ATM/POS transaction system.

27

28

29 **Summary of the Invention**

30 A preferred embodiment of the present invention
31 comprises a system for a purchaser to perform an on-
32 line ATM/POS financial transaction from a personal
33 computer over a public access communications network
34 utilizing a universally acceptable electronic financial
35 transaction instruction that debits a purchaser's
36 checking or savings account. The financial transaction

1 instruction is provided in a secured format for
2 transactions sent over the public access communications
3 network, which is external from an on-line ATM/POS
4 transaction system. The system of the present
5 invention utilizes card and security information to
6 authenticate the purchaser and validate their authority
7 to initiate the financial transaction instruction to
8 debit the identified account. Further, the system
9 utilizes a secure mechanism to protect the card and
10 security information as it is transmitted over the
11 public access network to a financial institution
12 providing access to the on-line ATM/POS transaction
13 system. The system of the present invention
14 advantageously does not require an account relationship
15 between the purchaser, the merchant, and the financial
16 institution providing access to the on-line ATM/POS
17 system. Further, the system beneficially does not
18 require the bank used by the purchaser and/or the bank
19 used by the merchant to have the capability to perform
20 financial transaction instructions over the Internet.
21 Additionally, the system is compatible with current
22 financial transaction systems, thus making the present
23 financial transaction instruction a universally
24 acceptable on-line ATM/POS transaction from a source
25 external from the on-line ATM/POS transaction system.

26
27 According to a preferred embodiment, a method of
28 performing a financial transaction between a purchaser
29 and a merchant, comprises creating purchaser payment
30 instructions comprising encrypted, electronic
31 representations of a purchaser transaction amount, card
32 information and security information. The card
33 information identifies a checking or savings account at
34 purchaser's bank and the security information comprises
35 a personal identification number associated with the
36 identified card number for authorizing its use in an

1 on-line ATM/POS transaction. The card information and
2 the security information must be encrypted, using an
3 encryption method dictated by on-line ATM/POS
4 transaction system standards. The purchaser payment
5 instructions are protected by a first secure mechanism,
6 such as encryption or digital signature. The digital
7 signature of the purchaser provides verification of the
8 identity of the purchaser and the integrity of the
9 purchaser payment instruction. The purchaser payment
10 instructions are electronically delivered to the
11 merchant, such as over a public access network like the
12 Internet. Merchant payment instructions are appended
13 to the purchaser payment instructions to create
14 financial transaction instructions. The merchant
15 payment instructions comprise merchant identification
16 and merchant deposit account identification used in
17 performing the transaction. The financial transaction
18 instructions are protected by a second secure
19 mechanism, such as with encryption and/or by the
20 digital signature of the merchant. The merchant's
21 digital signature provides verification of the
22 merchant's identity and of the integrity of the
23 financial transaction instructions. A digital
24 certificate of the merchant may be appended to the
25 financial transaction instructions, where the
26 merchant's digital certificate provides additional
27 verification of the merchant's identity and the
28 integrity of the financial transaction instructions.

29
30 The financial transaction instructions are
31 electronically delivered, such as over the Internet, to
32 a financial institution offering access to the on-line
33 ATM/POS transaction system to perform the financial
34 transaction. The financial institution removes and
35 reformats the encrypted financial transaction
36 instructions to form an ATM/POS transaction request.

1 Reformatting the information comprises placing the
2 ATM/POS transaction request in a form accepted by the
3 on-line ATM/POS transaction system. The ATM/POS
4 transaction request is electronically delivered to the
5 purchaser's bank through the on-line ATM/POS
6 transaction system. A response message is received at
7 the financial institution from the purchaser's bank
8 through the on-line ATM/POS transaction system, where
9 the response message is an approval if the financial
10 transaction is acceptable and a denial if the financial
11 transaction is unacceptable. An authorization message
12 is electronically delivered to the merchant to indicate
13 whether the response message is an approval or a
14 denial. If the response message is an approval, then
15 the identified account number is debited by the
16 transaction amount and a credit equivalent to the
17 transaction amount is sent to the merchant's deposit
18 account. Thus, the present invention provides a system
19 and method for a low cost, electronic financial
20 transaction instruction for an on-line ATM/POS
21 transaction from a source external from the on-line
22 ATM/POS transaction system utilizing checking or
23 savings account funds.

24
25

26 **Brief Description Of The Drawings**

27 Fig. 1 is a schematic representation of one
28 embodiment of a system according to the present
29 invention;

30 Figs. 2A-2C are flow charts representing one
31 embodiment of a method of the present invention;

32 Fig. 3 is a more detailed schematic representation
33 of a portion of the system of Fig. 1; and

34 Figs. 4A-4C are flow charts representing another
35 embodiment of a method of the present invention.

36

1 **Detailed Description Of The Invention**

2 The present invention comprises a system and
3 method for a purchaser to perform an on-line ATM/POS
4 transaction utilizing checking and savings account
5 funds from a transaction source external from the on-
6 line ATM/POS transaction system, such as a personal
7 computer connected to the Internet. According to one
8 preferred embodiment of the present invention,
9 referring to Fig. 1, a system 10 for performing a
10 financial transaction comprises a purchaser 12 remotely
11 interacting 13 with a merchant 14 over a communications
12 network 16, such as a public access network like the
13 Internet and its World Wide Web or electronic mail (e-
14 mail) protocols, and other similar networks. Purchaser
15 12 provides merchant 14 with digitally signed and/or
16 encrypted, electronic purchaser payment instructions
17 15. Purchaser payment instructions 15 include
18 encrypted card information and security information.
19 Merchant 14 adds merchant payment instructions 17, such
20 as merchant identification and transaction amount
21 information, to purchaser payment instructions 15 to
22 form an electronic financial transaction instruction 18
23 that the merchant digitally signs and/or encrypts.
24 Financial transaction instructions 18 thus comprise
25 data suitable for performing an on-line ATM/POS
26 transaction. Merchant 14 remotely transfers financial
27 transaction instruction 18 over communications network
28 20, which is similar or the same as communications
29 network 16, to a financial institution 22. In an
30 alternate embodiment, merchant 14 may send financial
31 transaction instruction 18 to a merchant service
32 provider that handles the merchant's financial
33 transactions, which then forwards the financial
34 transaction instruction to financial institution 22.
35 Financial institution 22 is a bank or other service
36 provider that provides purchaser 12 with indirect

1 access to the on-line ATM/POS transaction system 24,
2 such as the ATM network. As such, financial
3 institution 22 removes the data suitable for performing
4 an on-line ATM/POS transaction from financial
5 transaction instruction 18. Financial institution 22
6 formats the data into a standard ATM/POS transaction
7 request 26 and performs a standard ATM/POS transaction,
8 just like a transaction performed at an ATM or at a
9 merchant POS terminal.

10
11 As such, financial institution 22 sends
12 transaction request 26 to purchaser's bank 28 through
13 on-line ATM/POS transaction system 24. Purchaser's
14 bank 28 returns a response message 30 to financial
15 institution 22 comprising an authorization if
16 transaction request 26 is approved, or a denial if not
17 approved. Correspondingly, purchaser's bank 28 debits
18 an account identified in transaction request 26 if the
19 request is approved. Financial institution 22 notifies
20 merchant 14 of the approval status of the financial
21 transaction instruction 18 by sending an authorization
22 message 32 over network 20. Correspondingly, if the
23 transaction is approved, financial institution 22
24 provides merchant's bank 34 with a credit 36 through a
25 bank payment system network 38, such as the Automated
26 Clearing House (ACH). Upon receiving authorization
27 message 32, merchant 14 may then complete the
28 transaction, if required. As a result, purchaser 12
29 and merchant 14 perform a financial transaction with a
30 guaranteed payment that is authorized in real time and
31 on-line. Thus, the present invention provides a system
32 and method for an on-line ATM/POS transaction over a
33 public access network external from the on-line ATM/POS
34 transaction system.

35
36 Typically, on-line ATM/POS transactions are only

1 performed at sources that are directly connected to the
2 on-line ATM/POS transaction system through a hard-
3 wired, direct connection to an on-line ATM/POS service
4 provider, such as financial institution 22. The hard-
5 wired, direct connection is typically a private
6 telephone line that is leased from the service provider
7 or from the ATM/POS network provider. For example,
8 ATM's and merchant POS terminals are directly connected
9 to the on-line ATM/POS transaction system. As such,
10 access to the on-line ATM/POS network is generally
11 restricted to these sources.

12

13 In contrast, the present invention is a system
14 that provides on-line ATM/POS transaction capability
15 over a public access network or open network, such as
16 the Internet. The rise in commerce being performed
17 over public access networks with no direct connections
18 to, or that are external from, the on-line ATM/POS
19 system has created a new point-of-sale. One example of
20 such a new point of sale is a personal computer
21 connected to the Internet. These new points-of-sale,
22 however, are outside of the current paradigm for
23 connection to the on-line ATM/POS system. As a result,
24 reliable and secure methods for performing an on-line
25 ATM/POS transaction from these new POS sources are
26 lacking. Therefore, the present invention beneficially
27 allows a consumer the convenience of utilizing checking
28 or savings account funds in an on-line ATM/POS
29 transaction from a source that is remote from the on-
30 line ATM/POS system, such as the Internet, thereby
31 resulting in an external ATM/POS transaction that is
32 on-line and in real time.

33

34 As used herein, the term "purchaser" refers to an
35 entity that is exchanging value for a good, a service
36 or for other value. The purchaser is the owner of, or

1 rightfully has access to, the savings or checking
2 account that comprises the funds or value utilized by
3 the purchaser in the transaction. The term "merchant"
4 refers to an entity that is exchanging a good, a
5 service or value for the purchaser's value. Typically,
6 the purchaser is on a public access network, such as
7 the Internet, buying items from the merchant.
8 Although, as one skilled in the art will realize, many
9 other similar financial transactions may be performed
10 utilizing the present invention.

11

12 Financial transaction instruction 18, as is
13 discussed in more detail below, comprises all of the
14 data necessary to perform an on-line ATM/POS
15 transaction. Typically, this information comprises
16 information concerning the purchaser, the merchant and
17 the transaction. Purchaser information may comprise
18 name identification, a card number used as a source of
19 value for debiting, and a personal identification
20 number (PIN) for authenticating the purchaser for use
21 of the card number. The card number is then cross-
22 referenced to an account number within the systems of
23 purchaser's bank. Similarly, merchant information may
24 include name identification, and an account number for
25 crediting with value. Finally, transaction information
26 or purchase order information may comprise the
27 quantities, identification and prices of goods and
28 services, the transaction amount, the transaction date
29 and the transaction time, etc. All of this information
30 is typically contained in purchaser and merchant
31 payment instructions, as is discussed below.

32

33 Referring to Figs. 2A-2C and 3, a preferred system
34 10 of the present invention comprises purchaser 12
35 making a purchase from merchant 14, such as a purchaser
36 accessing a merchant's World Wide Web site with a

1 personal computer or other source that is external
2 from, or not directly connected to, the on-line ATM/POS
3 transaction system 24 (Fig. 2, Block 110). Upon
4 placing an order for an item from the site, purchaser
5 12 is presented with a number of payment options (Block
6 112). One of the payment options is to perform the
7 transaction utilizing funds from the purchaser's
8 checking or savings account. Upon selecting this
9 option (Block 114), purchaser 12 is prompted to provide
10 card information 39 (Fig. 3) and security information
11 40 (Fig. 3) to identify and authenticate themselves and
12 validate the transaction (Block 116).

13
14 Referring to Fig. 3, card information 39 is
15 contained in memory 42 on card 44, such as an ATM,
16 debit and smart card, or is contained within software
17 46 within memory 48 of computer 50 utilized by
18 purchaser 12. Computer 50, such as a personal computer
19 located at the purchaser's home or business, may
20 further comprise a processor 52 and an input/output 54
21 connected to communications network 16. Card
22 information 39 may comprise cardholder data 56, such as
23 the name of the cardholder, and card number data 58.
24 Card number data 58 includes a bank identification
25 number used to direct the transaction through on-line
26 ATM/POS system 24 (Fig. 1). Further, card number data
27 58 includes a number that is associated with the actual
28 savings or checking account number in purchaser's bank
29 28 to be used to fund the transaction. Also, card
30 information 39 may comprise any other type of data that
31 purchaser's bank 28 may choose to include in memory 42
32 as allowed by ISO standards. The ATM card comprises a
33 magnetic stripe that holds card information 39, while
34 the smart card contains similar information within an
35 embedded microcomputer. Additionally, security
36 information 40 comprises a secret number known by the

1 cardholder and the card issuer, such as a personal
2 identification number (PIN) 60. PIN 60 is a number
3 that is used by a cardholder to identify themselves to
4 their bank to authorize on-line ATM/POS transactions.
5

6 Purchaser 12 may enter card information 39 and
7 security information 40 by placing card 44 into
8 communication with card reader interface 62 of card
9 reader device 64 and by entering PIN 60 into keypad 66
10 of the card reader device. For example, the purchaser
11 may use a Citibank[®] ATM card and insert it into a
12 magnetic stripe reader/writer device. Alternatively,
13 the purchaser may use a Citibank[®] Smart Card and insert
14 it into a smart card reader/writer device, such as the
15 PC PAY[®] PC2200 product from Innovonics, Inc. of Phoenix,
16 Arizona. Card reader device 64 may further comprise a
17 processor 68 and a memory 70, including security
18 software 72 comprising encryption algorithms. Security
19 software 72 encrypts card information 39 and security
20 information 40 (Block 116) according to ATM/POS network
21 standards, which currently comprise encrypting the data
22 according to the Data Encryption Standard (DES). DES
23 is a symmetric encryption method where financial
24 institution 22 (Fig. 1) holds the decryption key.
25 Although, as one skilled in the art will realize, many
26 other encryption methods may be utilized. Card reader
27 device 64 forwards the encrypted card information 39
28 and security information 40 to computer 50, which may
29 also add other information to form purchaser payment
30 instructions 15 (Block 118). Purchaser payment
31 instructions 15 may comprise many other instructions,
32 such as purchase order information including the
33 quantity and price of the good/service and purchaser's
34 transaction amount, delivery information, authorization
35 to add shipping costs up to a specified limit,
36 authorizations to make payment in a foreign currency

1 while debiting the account in U.S. dollars, etc.

2
3 Additionally, secure mechanism 74 is an security
4 method utilized to protect purchaser payment
5 instructions 15 in the transfer to merchant 14 or any
6 other entity (Block 120) over communications network
7 16. Secure mechanism 74 provides integrity assurance,
8 verifying that purchaser payment instructions 15 have
9 not been altered, and also allows financial institution
10 22 to confirm the identity of purchaser 12. For
11 example, secure mechanism 74 may comprise one or a
12 combination of the following operations on purchaser
13 payment instructions 15: symmetric encryption,
14 asymmetric encryption, a purchaser's verifiable digital
15 signature and a verifiable digital certificate.
16 Although, as one skilled in the art will realize, many
17 other security methods may be utilized. Preferably,
18 purchaser payment instructions 15 are digitally signed
19 by purchaser 12. The digital signature of purchaser 12
20 verifies purchaser's identity and that purchaser
21 payment instructions 15 have not been altered. This
22 provides a first level of protection for transmitting
23 purchaser payment instructions 15 over communications
24 network 16. A digital certificate may also be used to
25 provide verification of the identity of the sender, as
26 well as providing the sender's public key for use in
27 sending an encrypted response back to the sender.

28
29 A second level of privacy and protection comprises
30 encrypting the digitally signed purchaser payment
31 instructions 15 before transmission to merchant 14.
32 Depending on the what kind of privacy is required, and
33 between which parties, this second level of privacy
34 provided by secure mechanism 74 may comprise any or a
35 combination of symmetric and asymmetric encryption.
36 For example, purchaser 12 may want or allow merchant 14

1 to have access to the portion of purchaser payment
2 instructions 15 comprising the purchase order
3 information. In this case, then an encryption method
4 is chosen that allows merchant 14 and financial
5 institution 22 the ability to decrypt this portion of
6 purchaser payment instructions 15. In this case,
7 however, financial institution 22 is still the only
8 party able to decrypt the encrypted card information 39
9 and security information 40 within purchaser payment
10 instructions 15. Alternatively, purchaser 12 may
11 encrypt the digitally signed purchase payment
12 instructions 15 in such a way so that decryption of
13 the whole purchaser payment instructions 15 may be
14 performed only by financial institution 22. Thus,
15 secure mechanism 74 provides a first level of
16 protection with the digital signature, and a further
17 level of protection and privacy with encryption of the
18 digitally signed purchaser payment instructions 15.
19 Therefore, purchaser 12 provides merchant 14 with
20 purchaser payment instructions 15 that comprise
21 optionally encrypted, digitally signed and DES
22 encrypted card information 39 and security information
23 40 utilized in an on-line ATM/POS transaction.

24
25 Merchant 14 appends merchant payment instructions
26 17 to purchaser payment instructions 15 to form
27 financial transaction instructions 18 (Block 122).
28 Merchant payment instructions 17 may comprise
29 information identifying merchant's bank 34 and
30 merchant's deposit account number for crediting, as
31 well as other similar merchant information related to
32 the transaction. Merchant payment instructions 17 may
33 also include purchase order information including
34 merchant's transaction amount, merchant identification
35 information, the currency to be utilized, etc. Secure
36 mechanism 76 (Fig. 1) is utilized to protect the

1 transmission of financial transaction instructions 18,
2 comprising the secure mechanism 74 protected purchaser
3 payment instructions 15 and merchant payment
4 instructions 17, over communications network 20.
5 Secure mechanism 76, similar to secure mechanism 74,
6 provides integrity assurance by verifying that
7 financial transaction instructions 18 have not been
8 altered, and also allows financial institution 22 to
9 confirm the identity of merchant 14. For example,
10 secure mechanism 76 may comprise one or a combination
11 of the following operations on financial transaction
12 instructions 18: symmetric encryption, asymmetric
13 encryption, a purchaser's verifiable digital signature
14 and a verifiable digital certificate. Although, as one
15 skilled in the art will realize, many other security
16 methods may be utilized. Preferably, financial
17 transaction instructions 18 are digitally signed by
18 merchant 14. The digital signature of merchant 14
19 verifies merchant's identity and that financial
20 transaction instructions 18 have not been altered.
21 This provides a first level of protection for
22 transmitting financial transaction instructions 18 over
23 communications network 20. Since there may be no
24 relationship between merchant 14 and financial
25 institution 22, a digital certificate may also be used
26 to provide verification of the identity of merchant 14,
27 as well as providing the merchant's public key for use
28 in sending an encrypted response back to the merchant.

29
30 A second level of privacy and protection comprises
31 encrypting the digitally signed financial transaction
32 instructions 18 before transmission to financial
33 institution 22. Since the digital signature of
34 financial transaction instructions 18 that includes
35 merchant payment instructions 17, such as the
36 merchant's account number, leaves the merchant payment

1 instructions in the clear, the merchant may have a
2 strong motivation to further protect the privacy of the
3 transaction. To further increase security, all or a
4 portion of financial transaction instructions 18 may be
5 encrypted by merchant 14 with a key preferably known
6 only by the merchant and financial institution 22.
7 Thus, similar to purchaser payment instructions 15,
8 financial transaction instructions 18 are protected by
9 secure mechanism 76 (Fig. 1) and transferred through
10 communications network 20 to financial institution 22
11 (Block 124).

12

13 Financial institution 22 receives the protected
14 financial transaction instructions 18 and decrypts them
15 (Block 126). Financial institution 22 then validates
16 financial transaction instructions 18, as well as
17 insuring that purchase order information, purchaser's
18 and merchant's transaction amount and other information
19 utilized in performing the transaction is in agreement
20 between purchaser 12 and merchant 14. As mentioned
21 above, the present invention advantageously does not
22 require any type of account relationship between
23 purchaser 12, merchant 14 and financial institution 22.
24 The purchaser 12 and/or merchant 14 only need to
25 exchange keys with financial institution 22 for
26 encryption/decryption purposes. Financial institution
27 22 then reformats card information 39 and security
28 information 40 into transaction request 26 that meets
29 the standard for an on-line ATM/POS transaction.
30 Transaction request 26 is routed through and processed
31 by on-line ATM/POS transaction system 24 (Block 128).
32 Typically, transaction request 26 is required to be
33 sent in an encrypted format over on-line ATM/POS
34 network 24 according to set standards. For example,
35 financial institution 22 such as Citibank[®] may route
36 transaction request 26 through Citishare[®], Citibank's

1 ATM/POS network interface. Financial institution 22
2 and on-line ATM/POS transaction system 24 thus treat
3 transaction request 26 as if it were an electronic
4 transaction initiated at a merchant POS terminal, an
5 ATM terminal or some other similar source directly
6 connected to on-line ATM/POS transaction system 24. By
7 formatting transaction request 26 as a typical on-line
8 ATM/POS transaction, the present invention allows
9 financial transaction instructions 18 to be universally
10 accepted by existing on-line ATM/POS financial
11 transaction networks. Thus, the settlement of
12 financial transaction instructions 18 follows the
13 standard procedure which is used for typical on-line
14 ATM/POS transactions.

15
16 Purchaser's bank 28 decrypts (if necessary)
17 transaction request 26 and verifies purchaser's card
18 information 39 and security information 40.
19 Additionally, purchaser's bank 28 performs a number of
20 other checks, such to determine whether or not the card
21 is stolen, the account is blocked, etc. Purchaser's
22 bank 28 then approves or disapproves the transaction
23 on-line and in real time, as it would any other on-line
24 ATM/POS transaction initiated at an ATM or a merchant
25 location (Block 130). Purchaser's bank 28 makes an
26 approval/disapproval decision by determining if the
27 account associated with card information 39 has
28 sufficient funds to cover the transaction amount
29 identified in transaction request 26. If approved,
30 then the transaction amount is reserved from the
31 identified account so that it is not available for
32 later transactions. Purchaser's bank sends the
33 approval/disapproval information in response message 30
34 to financial institution 22 through on-line ATM/POS
35 transaction system 24 (Block 132). Financial
36 institution 22 then sends authorization message 32 back

1 to merchant 14 in real time (Block 134). The term "real
2 time" preferably means a time in the range of about
3 seconds to about minutes, although it could be longer.
4 Preferably, the time period from initialization of the
5 transaction to the merchant receiving authorization
6 message 32 is real time. If approved, financial
7 institution 22 initiates a credit, using traditional
8 payment systems such as ACH system 38, to merchant's
9 account at merchant's bank 34 in accordance with the
10 instructions contained in merchant's payment
11 instructions 17 (Block 136). The settlement of
12 financial transaction instruction 18 typically occurs
13 at the end of the business day of the transaction, as
14 purchaser's account is debited and merchant's account
15 is credited. Thus, with real time verified funding and
16 confidence of a payment, a merchant is able to respond
17 within minutes to an order over the Internet comprising
18 a low cost financial transaction presented by a
19 purchaser on a personal computer utilizing checking or
20 savings account funds (Block 138).

21
22 Referring to Figs. 4A-4C, an e-mail method for
23 performing an on-line ATM/POS transaction similar to
24 that in Figs. 3A-3C is described. Rather than the
25 transaction being performed over a World Wide Web site,
26 however, in Figs. 4A-4C the transaction is performed
27 via e-mail. As such, the initiation of the transaction
28 is somewhat different. In performing an on-line
29 ATM/POS transaction using e-mail, the purchaser
30 accesses payment software in their computer that allows
31 them to utilize their checking and savings account in
32 an e-mail payment transaction (Block 210). The
33 software allows order information to be associated with
34 a selected payment option (Block 212). Once the
35 appropriate account is selected (Block 214), the
36 remainder of the method (Blocks 216-238) is basically

1 the same as the method in Figs. 3A-3C except that
2 communications network 16 (Fig. 1) between purchaser
3 and merchant and/or communications network 20 (Fig. 1)
4 between merchant and financial institution is
5 preferably e-mail.

6
7 The present invention advantageously allows any
8 consumer with a valid ATM card or smart card, issued by
9 any financial institution anywhere in the world, to
10 utilize their checking or savings account from a
11 personal computer in an on-line ATM/POS transaction
12 over the Internet. Because the present invention
13 provides a financial transaction instruction that can
14 be utilized with existing on-line ATM/POS transaction
15 systems, the option to perform a checking or savings
16 account transaction over the Internet is available to
17 anyone with a hardware device capable of reading
18 information from an ATM card or smart card and the
19 software to securely send the information over a public
20 access network to a financial institution providing
21 access to the on-line ATM/POS transaction system. The
22 present invention allows any consumer having a valid
23 ATM card or smart card to perform an electronic
24 financial transaction instruction, regardless of
25 whether or not their financial institution offers this
26 service. Therefore, the availability of Internet
27 transactions involving checking and savings accounts is
28 dramatically expanded to all consumers having ATM or
29 smart cards.

30
31 Additionally, the present system may also be
32 utilized for numerous other transactions involving
33 checking or savings accounts. For example, the present
34 system may be advantageously utilized to electronically
35 pay bills, transfer money between individuals, and to
36 perform business to business payments using the World

1 Wide Web, e-mail and all of the other Internet
2 protocols.

3
4 Although the invention has been described with
5 reference to these preferred embodiments, other
6 embodiments can achieve the same results. Variations
7 and modifications of the present invention will be
8 apparent to one skilled in the art and the following
9 claims are intended to cover all such modifications and
10 equivalents.
11

1 **Claims**

2

3 What is claimed is:

4

5 1. A method of performing a financial transaction
6 between a purchaser and a merchant, comprising:
7 creating an electronic financial transaction
8 instruction for performing an on-line ATM/POS
9 transaction over a first public access network, the
10 financial transaction instruction comprising card
11 information, security information and transaction
12 amount information suitable for performing the on-line
13 ATM/POS transaction, wherein the card information and
14 security information are encrypted according to ATM/POS
15 transaction system standards;

16 including card number data suitable for use in an
17 on-line ATM/POS transaction with the card information,
18 wherein the card number data is associated with a
19 checking or savings account in purchaser's bank for
20 funding the on-line ATM/POS transaction;

21 including personal identification number data
22 suitable for use in an on-line ATM/POS transaction with
23 the security information, wherein the personal
24 identification number data is associated with the card
25 number data to identify the purchaser and authorize use
26 of the card number data; and

27 protecting the financial transaction instruction
28 for transmission over the first public access network
29 by utilizing a first secure mechanism, wherein the
30 first secure mechanism provides verification of the
31 identity of the purchaser and the integrity of the
32 financial transaction instruction.

33

34 2. A method of performing a financial transaction
35 as recited in claim 1, wherein creating the financial
36 transaction instruction is performed on a personal

1 computer external from the on-line ATM/POS transaction
2 system.

3
4 3. A method of performing a financial transaction
5 as recited in claim 2, wherein the first secure
6 mechanism provides at least a first level of protection
7 comprising performing an operation on the financial
8 transaction instruction to provide verification of the
9 identity of the purchaser and the integrity of the
10 financial transaction instruction while leaving all of
11 the financial transaction instruction in the clear
12 except for the encrypted card information and security
13 information.

14
15 4. A method of performing a financial transaction
16 as recited in claim 3, wherein the first level of
17 protection comprises digitally signing the financial
18 transaction instruction with the digital signature of
19 the purchaser.

20
21 5. A method of performing a financial transaction
22 as recited in claim 3, wherein the first level of
23 protection comprises appending a digital certificate of
24 the purchaser to the financial transaction instruction.

25
26 6. A method of performing a financial transaction
27 as recited in claim 2, wherein the first secure
28 mechanism comprises encrypting the financial
29 transaction instruction.

30
31 7. A method of performing a financial transaction
32 as recited in claim 3, wherein the first secure
33 mechanism further comprises a second level of
34 protection including encrypting the financial
35 transaction instruction for secure transmission over
36 the first public access network.

1 8. A method of performing a financial transaction
2 as recited in claim 7, wherein the encrypting the
3 financial transaction for the second level of
4 protection comprises encrypting in a manner decryptable
5 by the merchant.
6

7 9. A method of performing a financial transaction
8 as recited in claim 7, wherein the encrypting the
9 financial transaction for the second level of
10 protection comprises encrypting in a manner decryptable
11 by a financial institution providing access to the on-
12 line ATM/POS transaction system.
13

14 10. A method of performing a financial
15 transaction as recited in claim 7, further comprising
16 transmitting the financial transaction instruction to a
17 financial institution providing access to the on-line
18 ATM/POS transaction system.
19

20 11. A method of performing a financial
21 transaction as recited in claim 10, further comprising
22 decrypting and verifying the financial transaction
23 instruction and creating an on-line ATM/POS transaction
24 request utilizing the card information, security
25 information and transaction amount information.
26

27 12. A method of performing a financial
28 transaction as recited in claim 11, wherein the
29 financial institution performs the decrypting and
30 verifying of the financial transaction instruction and
31 the creating the on-line ATM/POS transaction request.
32

33 13. A method of performing a financial
34 transaction as recited in claim 11, further comprising
35 transmitting the transaction request to purchaser's
36 bank over the on-line ATM/POS transaction system.

1 14. A method of performing a financial
2 transaction as recited in claim 13, further comprising
3 transmitting an authorization message indicating the
4 approval status of the transaction request.
5

6 15. A method of performing a financial
7 transaction as recited in claim 3, further comprising
8 transmitting the financial transaction instruction to
9 the merchant over the first public access network.
10

11 16. A method of performing a financial
12 transaction as recited in claim 15, wherein the first
13 public access network is the Internet.
14

15 17. A method of performing a financial
16 transaction as recited in claim 16, wherein the
17 Internet protocol is the World Wide Web.
18

19 18. A method of performing a financial
20 transaction as recited in claim 16, wherein the
21 Internet protocol is electronic mail.
22

23 19. A method of performing a financial
24 transaction as recited in claim 15, further comprising
25 appending merchant payment instructions to the
26 financial transaction instruction.
27

28 20. A method of performing a financial
29 transaction as recited in claim 19, further comprising
30 protecting the financial transaction instruction for
31 transmission over a second public access network by
32 utilizing a second secure mechanism, wherein the second
33 secure mechanism provides verification of the identity
34 of the merchant and the integrity of the financial
35 transaction instruction.
36

1 21. A method of performing a financial
2 transaction as recited in claim 20, wherein the second
3 secure mechanism provides at least a first type of
4 protection comprising performing an operation on the
5 financial transaction instruction to provide
6 verification of the identity of the purchaser and the
7 integrity of the financial transaction instruction
8 while leaving all of the financial transaction
9 instruction in the clear except for the encrypted card
10 information and security information.

11
12 22. A method of performing a financial
13 transaction as recited in claim 21, wherein the first
14 type of protection comprises digitally signing the
15 financial transaction instruction with the digital
16 signature of the merchant.

17
18 23. A method of performing a financial
19 transaction as recited in claim 21, wherein the first
20 type of protection comprises appending a digital
21 certificate of the merchant to the financial
22 transaction instruction.

23
24 24. A method of performing a financial
25 transaction as recited in claim 20, wherein the second
26 secure mechanism comprises encrypting the financial
27 transaction instruction.

28
29 25. A method of performing a financial
30 transaction as recited in claim 21, wherein the second
31 secure mechanism further includes a second type of
32 protection comprising encrypting the financial
33 transaction instruction for secure transmission over
34 the second public access network.

35
36 26. A method of performing a financial

1 transaction as recited in claim 25, wherein the
2 encrypting the financial transaction for the second
3 type of protection comprises encrypting in a manner
4 decryptable by a financial institution providing access
5 to the on-line ATM/POS transaction system.
6

7 27. A method of performing a financial
8 transaction as recited in claim 25, further comprising
9 transmitting the financial transaction instruction to a
10 financial institution providing access to the on-line
11 ATM/POS transaction system
12

13 28. A method of performing a financial
14 transaction as recited in claim 27, further comprising
15 decrypting and verifying the financial transaction
16 instruction and creating an on-line ATM/POS transaction
17 request utilizing the card information, security
18 information and transaction amount information.
19

20 29. A method of performing a financial
21 transaction as recited in claim 28, wherein the
22 financial institution performs the decrypting and
23 verifying of the financial transaction instruction and
24 the creating the on-line ATM/POS transaction request.
25

26 30. A method of performing a financial
27 transaction as recited in claim 27, further comprising
28 transmitting the transaction request to purchaser's
29 bank over the on-line ATM/POS transaction system.
30

31 31. A method of performing a financial
32 transaction as recited in claim 30, further comprising
33 transmitting to the merchant an authorization message
34 indicating the approval status of the transaction
35 request.
36

1 32. A method of performing a financial
2 transaction between a purchaser and a merchant,
3 comprising:

4 creating an electronic financial transaction
5 instruction for performing an on-line ATM/POS
6 transaction over a first public access network, the
7 financial transaction instruction comprising card
8 information, security information and transaction
9 amount information suitable for performing the on-line
10 ATM/POS transaction, wherein the card information and
11 security information are encrypted according to ATM/POS
12 transaction system standards;

13 including card number data suitable for use in an
14 on-line ATM/POS transaction with the card information,
15 wherein the card number data is associated with a
16 checking or savings account in purchaser's bank for
17 funding the on-line ATM/POS transaction;

18 including personal identification number data
19 suitable for use in an on-line ATM/POS transaction with
20 the security information, wherein the personal
21 identification number data is associated with the card
22 number data to identify the purchaser and authorize use
23 of the card number data; and

24 protecting the financial transaction instruction
25 for transmission over the first public access network
26 by utilizing a first secure mechanism, wherein the
27 first secure mechanism comprises a first level of
28 protection and a second level of protection, wherein
29 the first level of protection comprises performing an
30 operation on the financial transaction instruction to
31 provide verification of the identity of the purchaser
32 and the integrity of the financial transaction
33 instruction while leaving all of the financial
34 transaction instruction in the clear except for the
35 encrypted card information and security information,
36 and wherein the second level of protection comprises

1 encrypting the financial transaction instruction for
2 secure transmission over the first public access
3 network.
4

5 33. A method of performing a financial
6 transaction as recited in claim 32, wherein creating
7 the financial transaction instruction is performed on a
8 personal computer external from the on-line ATM/POS
9 transaction system.
10

11 34. A method of performing a financial
12 transaction as recited in claim 33, wherein the first
13 public access network is the Internet.
14

15 35. A method of performing a financial
16 transaction as recited in claim 34, wherein the
17 Internet protocol is the World Wide Web.
18

19 36. A method of performing a financial
20 transaction as recited in claim 34, wherein the
21 Internet protocol is electronic mail.
22

23 37. A method of performing a financial
24 transaction as recited in claim 33, wherein the first
25 level of protection comprises digitally signing the
26 financial transaction instruction with the digital
27 signature of the purchaser.
28

29 38. A method of performing a financial
30 transaction as recited in claim 33, wherein the first
31 level of protection comprises appending a digital
32 certificate of the purchaser to the financial
33 transaction instruction.
34

35 39. A method of performing a financial
36 transaction as recited in claim 33, further comprising

1 transmitting the financial transaction instruction to a
2 financial institution providing access to the on-line
3 ATM/POS transaction system.
4

5 40. A method of performing a financial
6 transaction as recited in claim 39, further comprising
7 decrypting and verifying the financial transaction
8 instruction and creating an on-line ATM/POS transaction
9 request utilizing the card information, security
10 information and transaction amount information.
11

12 41. A method of performing a financial
13 transaction as recited in claim 40, further comprising
14 transmitting the transaction request to purchaser's
15 bank over the on-line ATM/POS transaction system.
16

17 42. A method of performing a financial
18 transaction as recited in claim 41, further comprising
19 transmitting an authorization message indicating the
20 approval status of the transaction request.
21

22 43. A method of performing a financial
23 transaction between a purchaser and a merchant,
24 comprising:
25 creating an electronic purchaser payment
26 instruction for performing an on-line ATM/POS
27 transaction over a first public access network, the
28 purchaser payment instruction comprising card
29 information, security information and transaction
30 amount information suitable for performing the on-line
31 ATM/POS transaction, wherein the card information and
32 security information are encrypted according to ATM/POS
33 transaction system standards;
34 including card number data suitable for use in an
35 on-line ATM/POS transaction with the card information,
36 wherein the card number data is associated with a

1 checking or savings account in purchaser's bank for
2 funding the on-line ATM/POS transaction;

3 including personal identification number data
4 suitable for use in an on-line ATM/POS transaction with
5 the security information, wherein the personal
6 identification number data is associated with the card
7 number data to identify the purchaser and authorize use
8 of the card number data;

9 protecting the purchaser payment instruction for
10 transmission over the first public access network by
11 utilizing a first secure mechanism, wherein the first
12 secure mechanism comprises a first level of protection
13 and a second level of protection, wherein the first
14 level of protection comprises performing an operation
15 on the purchaser payment instruction to provide
16 verification of the identity of the purchaser and the
17 integrity of the purchaser payment instruction while
18 leaving all of the purchaser payment instruction in the
19 clear except for the encrypted card information and
20 security information, and wherein the second level of
21 protection comprises encrypting the purchaser payment
22 instruction for secure transmission over the first
23 public access network;

24 appending merchant payment instructions to the
25 purchaser payment instruction to form a financial
26 transaction instruction; and

27 protecting the financial transaction instruction
28 for transmission over a second public access network by
29 utilizing a second secure mechanism, wherein the second
30 secure mechanism provides verification of the identity
31 of the merchant and the integrity of the financial
32 transaction instruction.

33

34 44. A method of performing a financial
35 transaction as recited in claim 43, wherein creating
36 the financial transaction instruction is performed on a

1 personal computer external from the on-line ATM/POS
2 transaction system.

3

4 45. A method of performing a financial
5 transaction as recited in claim 44, wherein the first
6 public access network and the second public access
7 network is the Internet.

8

9 46. A method of performing a financial
10 transaction as recited in claim 45, wherein the
11 Internet protocol is the World Wide Web.

12

13 47. A method of performing a financial
14 transaction as recited in claim 45, wherein the
15 Internet protocol is electronic mail.

16

17 48. A method of performing a financial
18 transaction as recited in claim 43, wherein the first
19 level of protection comprises digitally signing the
20 financial transaction instruction with the digital
21 signature of the purchaser.

22

23 49. A method of performing a financial
24 transaction as recited in claim 43, wherein the first
25 level of protection comprises appending a digital
26 certificate of the purchaser to the financial
27 transaction instruction.

28

29 50. A method of performing a financial
30 transaction as recited in claim 43, wherein the second
31 secure mechanism provides at least a first type of
32 protection comprising performing an operation on the
33 financial transaction instruction to provide
34 verification of the identity of the purchaser and the
35 integrity of the financial transaction instruction
36 while leaving all of the financial transaction

1 instruction in the clear except for the encrypted card
2 information and security information.

3

4 51. A method of performing a financial
5 transaction as recited in claim 50, wherein the first
6 type of protection comprises digitally signing the
7 financial transaction instruction with the digital
8 signature of the merchant.

9

10 52. A method of performing a financial
11 transaction as recited in claim 50, wherein the first
12 type of protection comprises appending a digital
13 certificate of the merchant to the financial
14 transaction instruction.

15

16 53. A method of performing a financial
17 transaction as recited in claim 43, wherein the second
18 secure mechanism comprises encrypting the financial
19 transaction instruction.

20

21 54. A method of performing a financial
22 transaction as recited in claim 50, wherein the second
23 secure mechanism further includes a second type of
24 protection comprising encrypting the financial
25 transaction instruction for secure transmission over
26 the second public access network.

27

28 55. A method of performing a financial
29 transaction as recited in claim 54, wherein the
30 encrypting the financial transaction for the second
31 type of protection comprises encrypting in a manner
32 decryptable by a financial institution providing access
33 to the on-line ATM/POS transaction system.

34

35 56. A method of performing a financial
36 transaction as recited in claim 43, further comprising

1 transmitting the financial transaction instruction to a
2 financial institution providing access to the on-line
3 ATM/POS transaction system.
4

5 57. A method of performing a financial
6 transaction as recited in claim 56, further comprising
7 decrypting and verifying the financial transaction
8 instruction and creating an on-line ATM/POS transaction
9 request utilizing the card information, security
10 information and transaction amount information.
11

12 58. A method of performing a financial
13 transaction as recited in claim 57, further comprising
14 transmitting the transaction request to purchaser's
15 bank over the on-line ATM/POS transaction system.
16

17 59. A method of performing a financial
18 transaction as recited in claim 58, further comprising
19 transmitting an authorization message indicating the
20 approval status of the transaction request.
21

22 60. A system for a purchaser to perform a
23 financial transaction, comprising:
24 a financial institution having access to an on-
25 line ATM/POS transaction system for performing said
26 financial transaction as an on-line ATM/POS
27 transaction, said financial institution receiving an
28 electronic financial transaction instruction in a first
29 secured format from said purchaser sent over an
30 electronic public access network, said financial
31 transaction instruction comprising encrypted card
32 information and security information, wherein said card
33 information comprises identification of a checking or
34 savings account held by said purchaser to be debited in
35 said financial transaction and wherein said security
36 information comprises a personal identification number

1 known by said purchaser to authorize the use of said
2 card information in said on-line ATM/POS transaction,
3 and wherein said first secured format of said financial
4 transaction instruction guarantees the identity of said
5 purchaser and the integrity of said financial
6 transaction instruction.

7

Amendments to the claims have been filed as follows

What is claimed is:

1. A method of performing a financial transaction between a purchaser and a merchant, comprising:

creating an electronic financial transaction instruction for performing an on-line ATM/POS transaction over a first public access network, the financial transaction instruction comprising card information, security information and transaction amount information suitable for performing the on-line ATM/POS transaction, wherein the card information and security information are encrypted according to ATM/POS transaction system standards and delivered from the purchaser to the merchant;

including card number data suitable for use in an on-line ATM/POS transaction with the card information, wherein the card number data is associated with a checking or savings account in purchaser's bank for funding the on-line ATM/POS transaction;

including personal identification number data suitable for use in an on-line ATM/POS transaction with the security information, wherein the personal identification number data is associated with the card number data to identify the purchaser and authorize use of the card number data; and

protecting the financial transaction instruction for transmission over the first public access network by utilizing a first secure mechanism, wherein the first secure mechanism provides verification of the identity of the purchaser and the integrity of the financial transaction instruction.

2. A method of performing a financial transaction as recited in claim 1, wherein creating the financial transaction instruction is performed on a personal

1 computer external from the on-line ATM/POS transaction
2 system.

3
4 3. A method of performing a financial transaction
5 as recited in claim 2, wherein the first secure
6 mechanism provides at least a first level of protection
7 comprising performing an operation on the financial
8 transaction instruction to provide verification of the
9 identity of the purchaser and the integrity of the
10 financial transaction instruction while leaving all of
11 the financial transaction instruction in the clear
12 except for the encrypted card information and security
13 information.

14
15 4. A method of performing a financial transaction
16 as recited in claim 3, wherein the first level of
17 protection comprises digitally signing the financial
18 transaction instruction with the digital signature of
19 the purchaser.

20
21 5. A method of performing a financial transaction
22 as recited in claim 3, wherein the first level of
23 protection comprises appending a digital certificate of
24 the purchaser to the financial transaction instruction.

25
26 6. A method of performing a financial transaction
27 as recited in claim 2, wherein the first secure
28 mechanism comprises encrypting the financial
29 transaction instruction.

30
31 7. A method of performing a financial transaction
32 as recited in claim 3, wherein the first secure
33 mechanism further comprises a second level of
34 protection including encrypting the financial
35 transaction instruction for secure transmission over
36 the first public access network.

1 8. A method of performing a financial transaction
2 as recited in claim 7, wherein the encrypting the
3 financial transaction for the second level of
4 protection comprises encrypting in a manner decryptable
5 by the merchant.

6
7 9. A method of performing a financial transaction
8 as recited in claim 7, wherein the encrypting the
9 financial transaction for the second level of
10 protection comprises encrypting in a manner decryptable
11 by a financial institution providing access to the on-
12 line ATM/POS transaction system.

13
14 10. A method of performing a financial
15 transaction as recited in claim 7, further comprising
16 transmitting the financial transaction instruction to a
17 financial institution providing access to the on-line
18 ATM/POS transaction system.

19
20 11. A method of performing a financial
21 transaction as recited in claim 10, further comprising
22 decrypting and verifying the financial transaction
23 instruction and creating an on-line ATM/POS transaction
24 request utilizing the card information, security
25 information and transaction amount information.

26
27 12. A method of performing a financial
28 transaction as recited in claim 11, wherein the
29 financial institution performs the decrypting and
30 verifying of the financial transaction instruction and
31 the creating the on-line ATM/POS transaction request.

32
33 13. A method of performing a financial
34 transaction as recited in claim 11, further comprising
35 transmitting the transaction request to purchaser's
36 bank over the on-line ATM/POS transaction system.

1 14. A method of performing a financial
2 transaction as recited in claim 13, further comprising
3 transmitting an authorization message indicating the
4 approval status of the transaction request.
5

6 15. A method of performing a financial
7 transaction as recited in claim 3, further comprising
8 transmitting the financial transaction instruction to
9 the merchant over the first public access network.
10

11 16. A method of performing a financial
12 transaction as recited in claim 15, wherein the first
13 public access network is the Internet.
14

15 17. A method of performing a financial
16 transaction as recited in claim 16, wherein the
17 Internet protocol is the World Wide Web.
18

19 18. A method of performing a financial
20 transaction as recited in claim 16, wherein the
21 Internet protocol is electronic mail.
22

23 19. A method of performing a financial
24 transaction as recited in claim 15, further comprising
25 appending merchant payment instructions to the
26 financial transaction instruction.
27

28 20. A method of performing a financial
29 transaction as recited in claim 19, further comprising
30 protecting the financial transaction instruction for
31 transmission over a second public access network by
32 utilizing a second secure mechanism, wherein the second
33 secure mechanism provides verification of the identity
34 of the merchant and the integrity of the financial
35 transaction instruction.
36

1 21. A method of performing a financial
2 transaction as recited in claim 20, wherein the second
3 secure mechanism provides at least a first type of
4 protection comprising performing an operation on the
5 financial transaction instruction to provide
6 verification of the identity of the purchaser and the
7 integrity of the financial transaction instruction
8 while leaving all of the financial transaction
9 instruction in the clear except for the encrypted card
10 information and security information.

11
12 22. A method of performing a financial
13 transaction as recited in claim 21, wherein the first
14 type of protection comprises digitally signing the
15 financial transaction instruction with the digital
16 signature of the merchant.

17
18 23. A method of performing a financial
19 transaction as recited in claim 21, wherein the first
20 type of protection comprises appending a digital
21 certificate of the merchant to the financial
22 transaction instruction.

23
24 24. A method of performing a financial
25 transaction as recited in claim 20, wherein the second
26 secure mechanism comprises encrypting the financial
27 transaction instruction.

28
29 25. A method of performing a financial
30 transaction as recited in claim 21, wherein the second
31 secure mechanism further includes a second type of
32 protection comprising encrypting the financial
33 transaction instruction for secure transmission over
34 the second public access network.

35
36 26. A method of performing a financial

1 transaction as recited in claim 25, wherein the
2 encrypting the financial transaction for the second
3 type of protection comprises encrypting in a manner
4 decryptable by a financial institution providing access
5 to the on-line ATM/POS transaction system.

6
7 27. A method of performing a financial
8 transaction as recited in claim 25, further comprising
9 transmitting the financial transaction instruction to a
10 financial institution providing access to the on-line
11 ATM/POS transaction system

12
13 28. A method of performing a financial
14 transaction as recited in claim 27, further comprising
15 decrypting and verifying the financial transaction
16 instruction and creating an on-line ATM/POS transaction
17 request utilizing the card information, security
18 information and transaction amount information.

19
20 29. A method of performing a financial
21 transaction as recited in claim 28, wherein the
22 financial institution performs the decrypting and
23 verifying of the financial transaction instruction and
24 the creating the on-line ATM/POS transaction request.

25
26 30. A method of performing a financial
27 transaction as recited in claim 27, further comprising
28 transmitting the transaction request to purchaser's
29 bank over the on-line ATM/POS transaction system.

30
31 31. A method of performing a financial
32 transaction as recited in claim 30, further comprising
33 transmitting to the merchant an authorization message
34 indicating the approval status of the transaction
35 request.
36

1 32. A method of performing a financial
2 transaction between a purchaser and a merchant,
3 comprising:
4 creating an electronic financial transaction
5 instruction for performing an on-line ATM/POS
6 transaction over a first public access network, the
7 financial transaction instruction comprising card
8 information, security information and transaction
9 amount information suitable for performing the on-line
10 ATM/POS transaction, wherein the card information and
11 security information are encrypted according to ATM/POS
12 transaction system standards;
13 including card number data suitable for use in an
14 on-line ATM/POS transaction with the card information,
15 wherein the card number data is associated with a
16 checking or savings account in purchaser's bank for
17 funding the on-line ATM/POS transaction;
18 including personal identification number data
19 suitable for use in an on-line ATM/POS transaction with
20 the security information, wherein the personal
21 identification number data is associated with the card
22 number data to identify the purchaser and authorize use
23 of the card number data; and
24 protecting the financial transaction instruction
25 for transmission over the first public access network
26 by utilizing a first secure mechanism, wherein the
27 first secure mechanism comprises a first level of
28 protection and a second level of protection, wherein
29 the first level of protection comprises performing an
30 operation on the financial transaction instruction to
31 provide verification of the identity of the purchaser
32 and the integrity of the financial transaction
33 instruction while leaving all of the financial
34 transaction instruction in the clear except for the
35 encrypted card information and security information,
36 and wherein the second level of protection comprises

1 encrypting the financial transaction instruction for
2 secure transmission over the first public access
3 network.

4

5 33. A method of performing a financial
6 transaction as recited in claim 32, wherein creating
7 the financial transaction instruction is performed on a
8 personal computer external from the on-line ATM/POS
9 transaction system.

10

11 34. A method of performing a financial
12 transaction as recited in claim 33, wherein the first
13 public access network is the Internet.

14

15 35. A method of performing a financial
16 transaction as recited in claim 34, wherein the
17 Internet protocol is the World Wide Web.

18

19 36. A method of performing a financial
20 transaction as recited in claim 34, wherein the
21 Internet protocol is electronic mail.

22

23 37. A method of performing a financial
24 transaction as recited in claim 33, wherein the first
25 level of protection comprises digitally signing the
26 financial transaction instruction with the digital
27 signature of the purchaser.

28

29 38. A method of performing a financial
30 transaction as recited in claim 33, wherein the first
31 level of protection comprises appending a digital
32 certificate of the purchaser to the financial
33 transaction instruction.

34

35 39. A method of performing a financial
36 transaction as recited in claim 33, further comprising

1 transmitting the financial transaction instruction to a
2 financial institution providing access to the on-line
3 ATM/POS transaction system.
4

5 40. A method of performing a financial
6 transaction as recited in claim 39, further comprising
7 decrypting and verifying the financial transaction
8 instruction and creating an on-line ATM/POS transaction
9 request utilizing the card information, security
10 information and transaction amount information.
11

12 41. A method of performing a financial
13 transaction as recited in claim 40, further comprising
14 transmitting the transaction request to purchaser's
15 bank over the on-line ATM/POS transaction system.
16

17 42. A method of performing a financial
18 transaction as recited in claim 41, further comprising
19 transmitting an authorization message indicating the
20 approval status of the transaction request.
21

22 43. A method of performing a financial
23 transaction between a purchaser and a merchant,
24 comprising:
25 creating an electronic purchaser payment
26 instruction for performing an on-line ATM/POS
27 transaction over a first public access network, the
28 purchaser payment instruction comprising card
29 information, security information and transaction
30 amount information suitable for performing the on-line
31 ATM/POS transaction, wherein the card information and
32 security information are encrypted according to ATM/POS
33 transaction system standards;
34 including card number data suitable for use in an
35 on-line ATM/POS transaction with the card information,
36 wherein the card number data is associated with a

1 checking or savings account in purchaser's bank for
2 funding the on-line ATM/POS transaction;

3 including personal identification number data
4 suitable for use in an on-line ATM/POS transaction with
5 the security information, wherein the personal
6 identification number data is associated with the card
7 number data to identify the purchaser and authorize use
8 of the card number data;

9 protecting the purchaser payment instruction for
10 transmission over the first public access network by
11 utilizing a first secure mechanism, wherein the first
12 secure mechanism comprises a first level of protection
13 and a second level of protection, wherein the first
14 level of protection comprises performing an operation
15 on the purchaser payment instruction to provide
16 verification of the identity of the purchaser and the
17 integrity of the purchaser payment instruction while
18 leaving all of the purchaser payment instruction in the
19 clear except for the encrypted card information and
20 security information, and wherein the second level of
21 protection comprises encrypting the purchaser payment
22 instruction for secure transmission over the first
23 public access network;

24 appending merchant payment instructions to the
25 purchaser payment instruction to form a financial
26 transaction instruction; and

27 protecting the financial transaction instruction
28 for transmission over a second public access network by
29 utilizing a second secure mechanism, wherein the second
30 secure mechanism provides verification of the identity
31 of the merchant and the integrity of the financial
32 transaction instruction.

33

34 44. A method of performing a financial
35 transaction as recited in claim 43, wherein creating
36 the financial transaction instruction is performed on a

1 personal computer external from the on-line ATM/POS
2 transaction system.

3

4 45. A method of performing a financial
5 transaction as recited in claim 44, wherein the first
6 public access network and the second public access
7 network is the Internet.

8

9 46. A method of performing a financial
10 transaction as recited in claim 45, wherein the
11 Internet protocol is the World Wide Web.

12

13 47. A method of performing a financial
14 transaction as recited in claim 45, wherein the
15 Internet protocol is electronic mail.

16

17 48. A method of performing a financial
18 transaction as recited in claim 43, wherein the first
19 level of protection comprises digitally signing the
20 financial transaction instruction with the digital
21 signature of the purchaser.

22

23 49. A method of performing a financial
24 transaction as recited in claim 43, wherein the first
25 level of protection comprises appending a digital
26 certificate of the purchaser to the financial
27 transaction instruction.

28

29 50. A method of performing a financial
30 transaction as recited in claim 43, wherein the second
31 secure mechanism provides at least a first type of
32 protection comprising performing an operation on the
33 financial transaction instruction to provide
34 verification of the identity of the purchaser and the
35 integrity of the financial transaction instruction
36 while leaving all of the financial transaction

1 instruction in the clear except for the encrypted card
2 information and security information.

3

4 51. A method of performing a financial
5 transaction as recited in claim 50, wherein the first
6 type of protection comprises digitally signing the
7 financial transaction instruction with the digital
8 signature of the merchant.

9

10 52. A method of performing a financial
11 transaction as recited in claim 50, wherein the first
12 type of protection comprises appending a digital
13 certificate of the merchant to the financial
14 transaction instruction.

15

16 53. A method of performing a financial
17 transaction as recited in claim 43, wherein the second
18 secure mechanism comprises encrypting the financial
19 transaction instruction.

20

21 54. A method of performing a financial
22 transaction as recited in claim 50, wherein the second
23 secure mechanism further includes a second type of
24 protection comprising encrypting the financial
25 transaction instruction for secure transmission over
26 the second public access network.

27

28 55. A method of performing a financial
29 transaction as recited in claim 54, wherein the
30 encrypting the financial transaction for the second
31 type of protection comprises encrypting in a manner
32 decryptable by a financial institution providing access
33 to the on-line ATM/POS transaction system.

34

35 56. A method of performing a financial
36 transaction as recited in claim 43, further comprising

1 transmitting the financial transaction instruction to a
2 financial institution providing access to the on-line
3 ATM/POS transaction system.
4

5 57. A method of performing a financial
6 transaction as recited in claim 56, further comprising
7 decrypting and verifying the financial transaction
8 instruction and creating an on-line ATM/POS transaction
9 request utilizing the card information, security
10 information and transaction amount information.
11

12 58. A method of performing a financial
13 transaction as recited in claim 57, further comprising
14 transmitting the transaction request to purchaser's
15 bank over the on-line ATM/POS transaction system.
16

17 59. A method of performing a financial
18 transaction as recited in claim 58, further comprising
19 transmitting an authorization message indicating the
20 approval status of the transaction request.
21

22 60. A system for a purchaser to perform a
23 financial transaction, comprising:
24 a financial institution having access to an on-
25 line ATM/POS transaction system for performing said
26 financial transaction as an on-line ATM/POS
27 transaction, said financial institution receiving an
28 electronic financial transaction instruction in a first
29 secured format from said purchaser sent over an
30 electronic public access network, said financial
31 transaction instruction comprising encrypted card
32 information and security information, wherein said card
33 information comprises identification of a checking or
34 savings account held by said purchaser to be debited in
35 said financial transaction and wherein said security
36 information comprises a personal identification number

1 known by said purchaser to authorize the use of said
2 card information in said on-line ATM/POS transaction,
3 and wherein said first secured format of said financial
4 transaction instruction guarantees the identity of said
5 purchaser and the integrity of said financial
6 transaction instruction.
7





The
Patent
Office

53



Application No: GB 9901782.4
Claims searched: 1-60

Examiner: Dr. Andrew Glanfield
Date of search: 15 April 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4T (TBX)

Int Cl (Ed.6): G06F (17/60), G07F (7/10), G07G (1/14)

Other: ONLINE: EPODOC, JAPIO, WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	EP 0385400 A2 (ATALLA) see whole document.	1, 32
X	WO 95/26085 A1 (INNOVONICS) see whole document.	1-7, 15-18, 32-36, 43-49
X, P	US 5809143 (HUGHES) see whole document.	1-7, 9-14, 32-42, 60.
X	US 5351296 (NIOBRARA) see whole document.	1, 32

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family

A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.